AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplica

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with Instagram unique identifying number: 56292455546;
Instagram Name:ahmadabdullahalmahdi
That is stored at a premises controlled by Meta Platforms, Inc.

Case No. 25-M-326 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See attachment B

YOU ARE COMMANDED to execute this warrant on or before 2-12-25 *(not to exceed 14 days)*
❒ in the daytime 6:00 a.m. to 10:00 p.m. [X at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 1-29-25. 10:40 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Instagram account with username: ahmadabdullahalmahdi, Instagram Unique Identifying Number 56292455546, that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. a company headquartered in Menlo Park, CA.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any emails, messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 7, 2025. Meta is required to disclose the following information to the government for each account listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from November 1, 2024 to current date;

7. Privacy and account settings, including change history; and

8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the Account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from November 1, 2024 to current date;

C. All content, records, and other information relating to communications sent from or received by the Account from 11/1/2024 to current date; including but not limited to:

1. The content of all communications sent from or received by the Account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the Account, including dates and times,

methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the Account and other Instagram users from November 1, 2024, including but not limited to:

1. Interactions by other Instagram users with the Account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account from November 1, 2024 to current date; and

F. All location information, including location history, login activity, information geotags, and related metadata from November 1, 2024 to current date;

Meta is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §245(b)(2): Federally Protected Activities, 18 U.S.C. §875 (c): Interstate Threats, and 18 U.S.C. §1038(a): False Information and Hoaxes. those violations involving Zidan Abdallah and occurring after November 1, 2024, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

A. Communications between the user of the SUBJECT ACCOUNT and victims;

B. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

C. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

D. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney

support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with Instagram unique identifying number: 56292455546; Instagram Name: ahmadabdullahalmahdi That is stored at a premises controlled by Meta Platforms, Inc.

Case No. 25-M-326 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §245(b)(2)	Federally Protected Activities
18 U.S.C. §875(c)	Interstate Threats
18 U.S.C. §1038(a)	False Information and Hoaxes

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

AMY MENTZEL
Digitally signed by AMY MENTZEL
Date: 2025.01.28 15:09:09 -06'00'

Applicant's signature

Amy Mentzel, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 1-29-25

Stephen C. Dries

Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Amy Mentzel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account, that is stored at premises owned, maintained, controlled, or operated by Instagram, a social media services company headquartered at 1 Meta Way, Menlo Park, CA 94025. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Instagram to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent for the Federal Bureau of Investigation ("FBI"), where I have been employed since 2006. I am currently assigned to an FBI squad which investigates civil rights and public corruption crimes. I was previously assigned to FBI Human Trafficking and Crimes Against Children Task Forces in the FBI Milwaukee and Detroit Divisions. I primarily investigated human trafficking, child exploitation, and kidnapping cases.

3. I am a federal law enforcement officer under applicable provisions of the United States Code and under Rule 41(a) of the Rules of Criminal Procedure. I have received training and have experience in the enforcement of the laws of the United States, including preparation and presentation of search warrants, and in executing court-ordered search warrants.

4. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based upon my personal observations, my training and experience,

and information obtained from various law enforcement personnel and witnesses. I have not included each and every fact known to me concerning this

investigation. I have set forth only the facts that I believe are necessary for the limited purpose of establishing probable cause to conduct a search of and for the items described in Attachments A and B for evidence, contraband, and/or instrumentalities of the criminal conduct described herein. Additionally, unless otherwise indicated, wherever in this Affidavit I assert that an individual made a statement, that statement is described in substance herein and is not intended to be a verbatim recitation of such statement. Furthermore, unless otherwise indicated, all statements contained in this Affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that a violation of 18 U.S.C. §245(b)(2): Federally Protected Activities, 18 U.S.C. §875 (c): Interstate Threats, and 18 U.S.C. §1038(a): False Information and Hoaxes, have been committed, are being committed, AND/OR will be committed by Zidan Abdallah. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i) AND/OR is in . . . a district in which the provider . . . "is located or in which the wire or electronic communications, records, or other information are stored." 18 U.S.C. § 2711(3)(A)(ii).

BACKGROUND OF INVESTIGATION
DEFINITIONS AND TECHNICAL TERMS

7. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

8. Instant messaging (IM) is a collection of technologies that create the possibility of real-time text-based communication between two or more participants via the Internet. Instant messaging allows for the immediate transmission of communications, including immediate receipt of acknowledgment or reply.

9. The term "Internet" is defined as the worldwide network of computers, a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

10. The term "ISP" (Internet Service Provider), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

11. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to

the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

12. Log files are computer files containing information regarding the activities of computer users, processes/programs running on the system and the activity of computer resources such as networks, modems, and printers. Log files can be used to identify activities that occurred on a specific computer. Installation (or install or setup) of a program is the act and the effect of putting the program in a computer system so that it can be executed.

PROVIDER BACKGROUND

13. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

14. The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Data Policy," https://help.instagram.com/519522125107875; "Information for Law Enforcement," https://help.instagram.com/494561080557017; and "Help Center," https://help.instagram.com.

15. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the

user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

16. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

17. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

18. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

19. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also

"block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

20. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

21. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

22. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

23. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their

username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

24. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

25. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

26. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

27. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and

retains payment information, billing records, and transactional and other information when these services are utilized.

28. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Meta retains records of a user's search history and followed hashtags.

29. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

30. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

31. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

32. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

33. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

34. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, [[instant messages, emails, voicemails, photos, videos, and documents]] are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

35. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device

identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

36. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

37. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE

38. On December 23, 2024, security personnel at the University School of Milwaukee (USM), located in River Hills, Wisconsin, contacted the River Hills Police Department (RHPD) to report USM had received a bomb threat from telephone number 587-205-6694. RHPD was unable to ping the number and it was determined to be a "spoof" or fake number. USM was on Christmas break, but hockey games were scheduled to take place on school grounds that day.

39. USM security guard J.P. told officers with RHPD that the caller asked if he was speaking with USM and stated he was going to blow up the school. J.P. also advised RHPD that a threatening voicemail had been left with USM from 917-686-2997 on December 21, 2024. RHPD found this number associated with ABDALLAH in Franklin Police Department (FPD) and Mequon Police Department (MPD) reports. This phone number was also attributed to

ABDALLAH in police reports obtained from the University of California, Santa Barbara Police Department (UCSB). On December 22, 2024, ABDALLAH's father contacted UCSB stating that ABDALLAH had left him a voicemail from this number threatening to kill him.

40. On December 24, 2024, the USM Security Director, Chad Wagner, contacted RHPD to advise that another threatening voicemail to USM was found from 414-415-4374, a number that was not attributed to a caller or carrier. The voice in this voicemail sounded like ABDALLAH. ABDALLAH did not identify himself in this call. Wagner advised RHPD that ABDALLAH had been a student at USM, but he had been expelled due to behavior issues. ABDALLAH also previously threatened a female USM student.

41. In an interview on January 8, 2025, J.P. told your Affiant that during the threatening phone call on December 23, 2024, the caller asked if J.P. was a devil worshipper and stated he would destroy the school, and that he would blow up the school. The caller made comments about Christians and Jews and other statements related to religion. The bomb threat prompted J.P. to advise Wagner to contact RHPD and the school was "shut down."

42. J.P. told your Affiant that she believed the person who made the bomb threat and left the threatening voicemails at the school may be the same person due to the tone of the voicemails and religious undertones in the messages. J.P. provided your Affiant with the two recorded voicemails to USM from telephone number 917-686-2997 and 414-415-4374 in which the caller, who initially identifies himself as ABDALLAH, stated the following:

VOICEMAIL 1: DECEMBER 21, 2024, FROM 917-686-2997

43. (Unintelligible ("UI")) My name is Zidan Wesam (UI) Abdullah. I (UI) over you, I'm, I'm the (UI), I'm the caliph of this world, I've been with spiritual energy in this world. Your ps- your school, I'm de..I'm publicly declaring under God, your school is pathetic, its satanism, its

Jewi-Judaism, you guys are all bought and known, pathetic white people, soulless white people, that think they have any spiritual energy or power. You guys are all pathetic and useless. You guys understand you're my bitches. I'll step on you like my fucking end of my fucking shoe. You understand me? Whoever is listening to this fucking, uh-uh, call. I dare you to challenge me. I dare you to go against me, you fucking pussy. You fucking little bitch, (UI), you-you fucking cowards. You guys were so scared of people that you-you, powered in your own school and made your own secret organization. You fucking idiots. You pathetic fucking, you mother fuckers, you guys literally fuck your own mothers and masturbate to your children, you pedophilic, satanistic, disgusting mother fuckers, you disgusting bitches, disgusting Jewish b-bitches. Fuck you niggas bro. Dead ass, fuck you niggas, you niggas are fucking retarded as fuck, you niggas are fucking slow. You niggas think your smart brain beats (UI) making (UI). All right bro, let see what God's about to do to your dumb ass school you bitch ass niggas. You pussy ass niggas, fuck you bitch ass niggas. Fuck you, suck my dick, bitch. Literally, (UI) literally, suck it, just like you suck your own Dad's dick, most of you, fucking pussys, literally, fuck you niggas.

VOICEMAIL 2: DECEMBER 23, 2024, FROM 414-415-4374

44. You guys are all going to be ravaged. You guys are all going to be torn to bits like the animals you are. You fucking sick savages. Fuck you all. You fucking, stupid mother fuckers. You fucking animals, you demons. I am living proof that the devil has no power. If I, for this guy that just recorded this voicemail. If I took his mom and I fucked his mom, with um, a sword and then I killed her (UI) and chopped her head off. What would you do? What would you do? Mother fucker. Fucking pussys. You guys know exactly who I am. You guys know exactly who you fucked with. You guys know exactly what your about to get up your fucking asses, all of you.

STATEMENTS FROM A.F. AND M.J.

45. On January 6, 2025, A.F. contacted the Milwaukee FBI to advise that Instagram user "ahmadabdullahalmahdi" had posted videos or "stories" to Instagram threatening Jewish students and an Indian student. The poster, who appears in many of the videos was identified by USM students and parents as ABDALLAH. A.F. advised that in the videos, ABDALLAH stated, "I hate Jews so much I'm going to kill them all," and "we need to kill all the Jews."

46. Your Affiant reviewed the videos provided by A.F. In on of the videos, ABDALLAH threatens to rip the head off M.J. and calls her a "disgusting, evil Indian." He states several times in the video that he will kill M.J. and if he sees her, he will "have to take her life." In another video ABDALLAH vehemently states "It's time for the Jews to die and the Indians to die."

47. On January 6, 2025, M.J. contacted the UC Santa Barbara Police Department ("UCSB") to report that she received direct messages from "ahmadabdullahalmahdi" via Instagram Messenger, who M.J. knew to be ABDALLAH. The police report states ABDALLAH messaged, "I'm going to kill you…You will die…Indian." ABDALLAH also posted a video to the Instagram account stating he would "slice your fucking head off your body" and called M.J. an "Indian slut." M.J. told an officer that she had attended school with ABDALLAH at USM, but they were not friends and did not really know each other. ABDALLAH made at least four videos posted on Instagram threatening to kill M.J. On January 6, 2025, ABDALLAH was served with an Emergency Protective Order ("EPO") for M.J. When served with the order, ABDALLAH stated to the officer, "It doesn't matter either because if she's gonna be killed she's gonna be killed with me and my army." The officer noted that a later Instagram story on ABDALLAH's account contained a video of the EPO torn into pieces. On Monday, January 6, 2025, UCSB arrested ABDALLAH for state violations of criminal trespass and stalking.

OTHER THREATS FROM 917-686-2997 AND INSTAGRAM

48. A UCSB missing person report for ABDALLAH, dated December 18, 2024, listed 917-686-2997, as the contact number for ABDALLAH. The report was made by ABDALLAH's father, who resides in Wisconsin. ABDALLAH's father made the report after ABDALLAH had not contacted his father for several hours after sending threatening text messages to his father and other family members. An additional December 18, 2024, UCSB report stated that these text messages to ABDALLAH's father and family members were sent between December 16 and December 18, 2024, and included, "I'm going to rape and destroy you," "Either serve me or die," and "If you do not serve me, its time for you to die."

49. A Santa Barbara County Sheriff's Department (SBCSD) report dated December 23, 2024, also associates phone number 917-686-2997 with ABDALLAH. ABDALLAH was arrested for vandalism and the assault of a security guard at a marijuana dispensary in Isla Vista, California.

50. On January 6, 2025, former USM student, H.L., made a complaint to the Mequon Police Department (MPD) regarding threats by ABDALLAH. H.L. stated that ABDALLAH made threats to H.L. and others, on Instagram stories. In a video, ABDALLAH stated, "Keep in mind that [H.L.'s first and last name] already knows he is going to die, he already knows I'm gonna kill him. He's gonna bow to me and he is gonna die." The MPD report also stated that ABDALLAH posted images showing his admiration for Luigi Mangione, who is a suspect criminally charged in a homicide in an allegedly planned assassination.

51. A compilation of numerous ABDALLAH Instagram videos and postings from USM parents was provided by USM on January 16, 2025. The videos were identified by USM and parents of USM students, after USM sent notification emails to the parents after the December 23, 2024, bomb threat. Your Affiant has viewed recent booking photos from California of

ABDALLAH, and ABDALLAH does appear in numerous undated videos in which he references killing Jews and crucifying "so many of you." There is a photo of four female USM students, and the three who are known to be Jewish have their faces crossed out with the word "Death" above them. In one video ABDALLAH states that anyone who challenges him will be killed. "I have to kill you. I have to kill somebody. Somebody has to die." ABDALLAH stated, "We need to kill all the Jews so I can get to Heaven." In other videos ABDALLAH stated he will masturbate to people dying and Jews dying. ABDALLAH mentions several USM students who are Jewish and threatens to kill them.

REQUEST TO MAINTAIN ACCOUNTS

52. Request to Maintain Account: I would further request the Court to order the Target Providers to continue to maintain the account(s) listed in Attachment A in an open and active status for one year from the date of this warrant so as not to disrupt this ongoing investigation.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

53. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

54. Based on the foregoing, I request that the Court issue the proposed search warrant.

55. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta Platforms, Inc.. Because the warrant will be served on Meta Platforms, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Instagram account with username: ahmadabdullahalmahdi, Instagram Unique Identifying Number 56292455546, that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. a company headquartered in Menlo Park, CA.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any emails, messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 7, 2025. Meta is required to disclose the following information to the government for each account listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from November 1, 2024 to current date;

7. Privacy and account settings, including change history; and

8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the Account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from November 1, 2024 to current date;

C. All content, records, and other information relating to communications sent from or received by the Account from 11/1/2024 to current date; including but not limited to:

1. The content of all communications sent from or received by the Account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the Account, including dates and times,

methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the Account and other Instagram users from November 1, 2024, including but not limited to:

1. Interactions by other Instagram users with the Account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account from November 1, 2024 to current date; and

F. All location information, including location history, login activity, information geotags, and related metadata from November 1, 2024 to current date;

Meta is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §245(b)(2): Federally Protected Activities, 18 U.S.C. §875 (c): Interstate Threats, and 18 U.S.C. §1038(a): False Information and Hoaxes. those violations involving Zidan Abdallah and occurring after November 1, 2024, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

A. Communications between the user of the SUBJECT ACCOUNT and victims;

B. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

C. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

D. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney

support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.